



ABSTRACT OF THE INVENTION

In situations where cryptographic systems need to protect two keys, and one key is less secure than the other, this invention provides a method of linking the two keys together which can detect the unauthorized modification of the less secure key. The more secure key is split or shared among multiple owners, such that a predetermined number of owners are required to expose this key. The exposure of the less secure key requires fewer owners. This invention uses several techniques to accomplish this, including encrypting the less secure key with the more secure key, or creating a message digest incorporating both keys, or using symmetric message integrity check of the less secure key using the more secure key.

10

20206.33